

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. EHAMA et al
Serial No.: Not Yet Assigned
Filed: March 17, 2004
Title: SECURITY SYSTEM

LETTER CLAIMING RIGHT OF PRIORITY

Mail Stop: Patent Applications
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

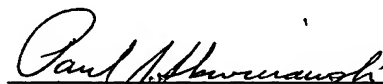
March 17, 2004

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicants hereby claim the right of priority based on **Japanese** Patent Application No. **2003-072919**, filed March 18, 2003.

A certified copy of said **Japanese** Application is attached.

Respectfully submitted,
ANTONELLI, TERRY, STOUT & KRAUS, LLP



Paul J. Skwierawski
Registration No. 32,173

PJW/dks
Attachment
(703) 312-6600

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月18日
Date of Application:

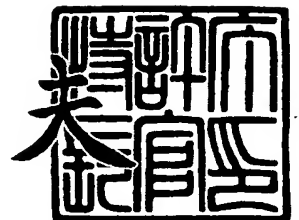
出願番号 特願2003-072919
Application Number:
[ST. 10/C]: [JP 2003-072919]

出願人 株式会社ルネサステクノロジ
Applicant(s):

2003年12月 4日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



【書類名】 特許願

【整理番号】 K03001021A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 江浜 真和

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 田中 和彦

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 細木 浩二

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 中田 啓明

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティシステム

【特許請求の範囲】

【請求項 1】

演算を行うプロセッサコアと、外部バスと接続するための外部バスインターフェースと、ローカルメモリへのアクセスを制御するメモリインターフェースと、前記プロセッサコアと前記外部バスインターフェースと前記メモリインターフェースとを接続する内部バスとを有する半導体装置であって、

前記外部バスインターフェースは、前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定する T L B と、前記プロセッサコアからの要求により T L B を書き換える T L B 制御回路を有し、

前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否か問い合わせる T L B 判定信号を前記 T L B へ送信し、

前記 T L B は、前記リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示す T L B 合否信号をアクセス制御回路へ返答し、

前記アクセス制御回路は、前記 T L B 合否信号がアクセス可であることを示している場合、前記内部バスへアクセスを許可し、前記 T L B 合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とする半導体装置。

【請求項 2】

請求項 1 記載の半導体装置であって、

前記 T L B 制御回路は、前記プロセッサコアが出力する T L B 更新要求に基づき、前記アクセス可能範囲を変更可能であることを特徴とする半導体装置。

【請求項 3】

請求項 1 記載の半導体装置であって、

前記外部バスは、P C I バスであることを特徴とする半導体装置。

【請求項 4】

請求項 1 記載の半導体装置であって、
前記外部バスは、汎用バスであることを特徴とする半導体装置。

【請求項 5】

請求項 1 記載の半導体装置であって、
前記内部バスに接続され、暗号処理を行う暗号演算回路をさらに有し、
前記アクセス制御回路は、当該暗号演算回路の秘密鍵や暗号処理方法を決定するレジスタへのアクセスを制限することを特徴とする半導体装置。

【請求項 6】

請求項 1 記載の半導体装置であって、
前記アクセス制御回路は、前記 T L B 合否信号がアクセス可であることを示している場合、前記内部バス、前記メモリインタフェースを介して前記ローカルメモリへのアクセスを許可することを特徴とする半導体装置。

【請求項 7】

外部バスに接続された半導体装置におけるバスインターフェース装置であって、
前記半導体装置内の内部バスに接続され、
前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定する T L B と、前記プロセッサコアからの要求により T L B を書き換える T L B 制御回路を有し、
前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否か問い合わせる T L B 判定信号を前記 T L B へ送信し、
前記 T L B は、前記リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示す T L B 合否信号をアクセス制御回路へ返答し、
前記アクセス制御回路は、前記 T L B 合否信号がアクセス可であることを示している場合、前記内部バスへアクセスを許可し、前記 T L B 合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とするバスインタフェース装置。

【請求項 8】

請求項 7 記載のバスインターフェース装置であって、
外部バスからアクセスされたアドレスを内部バスで用いるためのアドレスに変換するデコーダを有し、

前記アクセス制御回路は、前記デコーダで変換されたアドレスを用いて内部バスへリクエストを送信することを特徴とするバスインターフェース装置。

【請求項 9】

請求項 7 記載のバスインターフェース装置であって、

前記半導体装置内部の所定のアドレス空間がアクセス可能であることを示す許可ビット群を格納したレジスタと、前記外部からのアクセスが示すアドレスが当該半導体装置内部のアクセス可能な領域のアドレスか否かを判定するアクセス判定装置を有し、

前記アクセス判定回路は、前記デコーダと当該デコーダに接続されたセレクトを備え、

前記デコーダで変換されたアドレスから領域選択信号を生成し、前記許可ビット群のレジスタから出力される許可ビット信号と、前記領域選択信号を比較し、

前記領域選択信号と、前記許可ビット信号とが一致した場合は、アクセスが可能であることを示す前記アクセス合否信号を出力し、

前記領域選択信号と、前記許可ビット信号とが一致しない場合は、アクセスが否であることを示す前記アクセス合否信号を出力することを特徴とするバスインターフェース装置。

【請求項 10】

請求項 7 記載のバスインターフェース装置であって、

前記許可ビット群に格納されたデータの更新を行う許可ビット制御回路をさらに有し、

前記許可ビット制御回路は、内部バスを介して送信される書き換え要求信号に基づき、前記許可ビット群に格納されたデータを変更可能であることを特徴とするバスインターフェース装置。

【請求項 11】

記憶装置が接続された第 1 の半導体装置、第 2 の半導体装置、前記第 1 の半導体装置と前記第 2 の半導体装置を接続する外部バスとを有するコンピュータシステムであって、

前記第 1 の半導体装置は、

演算を行うプロセッサコアと、前記外部バスに接続されるための外部バスインターフェースと、前記記憶装置へのアクセスを制御するメモリインターフェースと、前記プロセッサコアと前記外部バスインターフェースと前記メモリインターフェースとを接続する内部バスとを有し、

前記第 2 の半導体装置から前記記憶装置へのアクセスがあった場合、

前記第 1 の半導体装置は、該アクセスのアドレスが、当該第 1 の半導体装置内の T L B に予め設定されたアクセス許可範囲内のアドレスか否かを判断し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バスを介して前記記憶装置へのアクセスを許可し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれない場合、前記アクセスを破棄し前記記憶装置へのアクセスを許可しないことを特徴とするコンピュータシステム。

【請求項 1 2】

請求項 1 1 記載のコンピュータシステムであって、

前記外部バスインターフェースは、前記外部バスからのリクエストを受けるアクセス制御回路と、前記アクセス制御回路に接続され前記外部バスアクセスの可否を判定する T L B と、前記プロセッサコアからの要求により T L B を書き換える T L B 制御回路を有し、

前記外部バスからのリクエストを受けたアクセス制御回路は、該リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否か問い合わせる T L B 判定信号を前記 T L B へ送信し、

前記 T L B は、前記リクエストのアドレスが、前記 T L B 内に設定されたアクセス許可範囲内のアドレスか否かを検索し、アクセス可否を示す T L B 合否信号をアクセス制御回路へ返答し、

前記アクセス制御回路は、前記 T L B 合否信号がアクセス可であることを示し

ている場合、前記内部バスへアクセスを許可し、前記 T L B 合否信号がアクセス否であることを示している場合、前記リクエストを破棄することを特徴とするコンピュータシステム。

【請求項 1 3】

任意の機能を有するモジュールと、外部バスに接続されるための外部バスインターフェースと、前記モジュールと前記外部バスインターフェースとを接続する内部バスとを有する半導体装置であって、

前記外部バスに接続される他の装置から前記モジュールへのアクセスがあった場合、

前記半導体装置は、該アクセスのアドレスが、当該半導体装置内の T L B に予め設定されたアクセス許可範囲内のアドレスか否かを判断し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バスを介して前記モジュールへのアクセスを許可し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれない場合、前記アクセスを破棄し前記記憶装置へのアクセスを許可しないことを特徴とする半導体装置。

【請求項 1 4】

請求項 1 3 記載の半導体装置であって、

当該半導体装置には記憶装置が接続されており、
前記記憶装置へのアクセスを制御するメモリインターフェースをさらに有し、

前記アクセスのアドレスが、前記アクセス許可範囲内のアドレスに含まれる場合、前記内部バス、前記メモリインタフェースを介して前記記憶装置へのアクセスを許可することを特徴とする半導体装置。

【発明の詳細な説明】

【 0 0 0 1】

【発明の属する技術分野】

本発明は外部バスインターフェースにてプロセッサ内部の機密情報を保護することのできるマイクロプロセッサに関する。

【 0 0 0 2】

【従来の技術】

特許文献1では、メモリへのデータアクセスを制限するためにメモリインターフェース回路とメモリの間にセキュリティ回路を設け、正しい手順でメモリアクセスが行われているかを監視している。このセキュリティ回路には鍵アドレスが設けてあり、この鍵アドレスに対応する特定の手順でアクセスが発生することで、メモリ空間へアクセス可能な範囲を拡大したり、予測するメモリアクセスからは使用しないメモリ空間を保護しデータ転送が実行されないようにすることが可能であった。また、メモリ保護機能が解除されていないアドレスに対してのアクセスが発生した場合、読み出されたデータの保障は行われえないという提案であった。

【0003】**【特許文献1】**

特開 2001-306400号公報

【0004】**【発明が解決しようとする課題】**

従来は外部メモリ空間のみの保護機能であり、プロセッサ内部メモリのデータに関しては保障されない。また、プロセッサ内部のメモリ空間全てにこの機能を搭載したとすると冗長論理が増大し、プロセッサの肥大化を招いてしまう。

【0005】

また、メモリ空間に対するアドレスの発行順序によって、メモリ保護の可否をハードウェアで行うため、汎用性に乏しい。

【0006】

また、保護機能を持たないプロセッサでは、外部バスからプロセッサ内部のレジスタやローカルメモリの読み出しや改変が可能であったため、暗号鍵などの機密データが閲覧されたり、開発したソフトウェアがコピーされてしまう可能性があった。

【0007】

本発明はこのような問題を鑑みてなされたものであり、プロセッサが外部デバイスと通信する汎用バスを用いた不正アクセス防止を目的とする。

【0008】**【課題を解決するための手段】**

この発明に係るプロセッサは、P C Iバスなどのプロセッサ外部の汎用バスとプロセッサの内部バスの中でデータ転送を制御するアクセス制御装置と、アクセスできる範囲が格納されているT L Bと、T L Bの内容を更新するT L B制御回路を具備する。

【0009】

プロセッサ内部からのアクセスによってのみT L Bを更新するT L B制御回路によってT L Bの内容を更新し、その更新した内容はP C Iバスなどのプロセッサ外部の汎用バスからのアクセスによって、アクセス制御回路から参照される。

【0010】

アクセス制御回路からのリクエストによりT L Bはアクセス可能領域であるかどうかをアクセス制御回路へ返答し、その結果によって、内部バスへリクエストを出すか、破棄するかを決定し、プロセッサ内部の機密情報を保護する。

【0011】**【発明の実施の形態】**

本発明の実施例について図面を参照して説明する。図1に本発明を適用したコンピュータシステムの構成例を示す。なお簡略化のため、本発明の適用と直接関係のない部分は省略する。

【0012】

メインC P U 1と高速バスインターフェースを持つノースブリッジ3へプロセッサバス2を用いて接続する。ノースブリッジ3は主記憶装置5とメモリバス4で接続し、また低速バスインターフェースを持つサウスブリッジ7とブリッジ間接続バス6を用いて接続する。

【0013】

サウスブリッジ7からP C Iバス8へ接続され、P C Iバス8上にメディアプロセッサ100 a、100 bを2個接続している。各々のメディアプロセッサ100 a、100 bはそれぞれローカルメモリ201 a、201 bへローカルメモリバス200 a、200 bを用いて接続する。また、フラッシュメモリ203 a

、203bへフラッシュメモリバス202a、202bを用いて接続する。尚、本実施例のメディアプロセッサ及びそれに相当する部分は1チップで構成されるが、複数チップにて実現することも可能である。

【0014】

メディアプロセッサ100a内部は内部バス109を用いて、演算を行うプロセッサコア101、PCIバス8と接続するためのPCIバスインターフェース102、プロセッサコア101の演算補助を行うコプロセッサ103、ローカルメモリへのアクセスを制御するメモリインターフェース104、I/Oインターフェースを制御するI/Oインターフェース105、暗号処理を行う暗号処理演算回路108が接続されている。暗号処理としては、Multi2/DES等がある。また、コプロセッサ103にコプロセッサ用メモリバス107を用いてコプロセッサ用メモリ106へ接続されている。

【0015】

さらに、PCIバスインターフェース102は動作設定を行うためのPCIバスインターフェースPIOレジスタ116を、プロセッサコア101はプロセッサコアPIOレジスタ117を、コプロセッサ103はコプロセッサPIOレジスタ118を、メモリインターフェース104はメモリインターフェースPIOレジスタ119を、I/Oインターフェース105はI/OインターフェースPIOレジスタ120を、暗号処理演算回路108は暗号処理演算回路PIOレジスタ121を、それぞれ持っている。

【0016】

メディアプロセッサ100aのブート時、I/Oインターフェース105がフラッシュメモリ203aからプログラムをロードし、内部バス109を通してプロセッサコア101がそのプログラムを実行することで、まずPCIバスインターフェース102内のTLB制御回路112へTLB書き換えリクエストを発生する。そのリクエストに応じてTLB制御回路112はTLB更新信号115をTLB111へ出すことでTLB111内部を変更し、起動時アクセス可能であったプロセッサ内部と、メディアプロセッサ100aの持つローカルメモリ201aとフラッシュメモリ203aの全領域のうち、ある特定の領域のみをアクセ

スできるようにする。

【0017】

メインCPU1からメディアプロセッサ100aへのリードアクセスが発生した場合には、そのリクエスト信号はノースブリッジ3、サウスブリッジ7へと送られ、PCIバス8を通してメディアプロセッサ100a内部のPCIバスインターフェース102が受ける。リクエスト信号を受けたアクセス制御回路110は、リードするアドレスがアクセス可能であるかどうかをTLB111へTLB判定信号113を通して問い合わせる。その信号を受け取ったTLB111は設定されているアドレスと比較し、その合否をTLB合否信号114を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス109へリクエストを出し、目的のデータを引き出し、PCIバス8を通してサウスブリッジ7、ノースブリッジ3を経由しメインCPUへとデータを返す。しかし、アクセスできない領域へのリードリクエストであった場合にはアクセス制御回路110は不定のデータをメインCPU1へ返す。

【0018】

また、ライトリクエストがメインCPU1からメディアプロセッサ100aへ出された場合、リードリクエストと同じ経路でPCIバスインターフェース102へと送られる。ライトリクエストを受け取ったアクセス制御回路110は、ライトするアドレスがアクセス可能であるかどうかをTLB111へTLB判定信号113を通して問い合わせる。その信号を受け取ったTLB111は内部のアドレスと比較し、その合否をTLB合否信号114を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合であり、内部バス109へリクエストを出し、書き換えを行う。しかし、アクセスできない領域へのライトリクエストであった場合にはアクセス制御回路110はその要求を破棄する。

【0019】

さらに、他のPCIデバイスであるメディアプロセッサ100bからのリードリクエストやライトリクエストも、メインCPU1からのアクセスと同様に判定が行われアクセス制限が行われる。

【0020】

特に、TLB111の変更はプロセッサコア101からのみ変更可能であり、メインCPU1や他のPCIデバイスからの変更は一切行うことができない。

【0021】

図2は汎用バスインターフェース123を持つメディアプロセッサ126の構成図である。汎用バスインターフェースとはアドレスバスとデータバス、リクエストなどの制御信号を持つバスである。リードリクエストとアドレスを発行することでデータバスに、要求したアドレスのデータを得ることができ、また、ライトリクエストとアドレスを発行し、データバスに書き込むデータを送信することで、変更するアドレスのデータを書き換えることができる。

メディアプロセッサ126は内部バス109を持ち、その内部バス109にプロセッサコア101、コプロセッサ103、メモリインターフェース104、I/Oインターフェース105、暗号処理演算回路108、汎用バスインターフェース123が接続されている。コプロセッサ103はコプロセッサ用メモリバス107を用いてコプロセッサ用メモリ106へ接続、メモリインターフェース104はローカルメモリバス200を用いてローカルメモリ201へ接続、I/Oインターフェース105はフラッシュメモリバス202を用いてフラッシュメモリ203へ接続している。

【0022】

さらに、汎用バスインターフェース123は動作設定を行うための汎用バスインターフェースPIOレジスタ116を、プロセッサコア101はプロセッサコアPIOレジスタ117を、コプロセッサ103はコプロセッサPIOレジスタ118を、メモリインターフェース104はメモリインターフェースPIOレジスタ119を、I/Oインターフェース105はI/OインターフェースPIOレジスタ120を、暗号処理演算回路108は暗号処理演算回路PIOレジスタ121を、それぞれ持っている。

【0023】

メディアプロセッサ126がブートすることで、フラッシュメモリ203からI/Oインターフェース105がブートプログラムを内部バス109を通してブ

ロセッサコア101へ送る。そのプログラムによってプロセッサコア101より内部バス109を用いてTLB制御回路112へTLB書き換えリクエストを発生し、汎用バスインターフェース123内のTLB111を更新する。その更新によって、起動時アクセス可能であったプロセッサ内部と、メディアプロセッサ102の持つローカルメモリ201とフラッシュメモリ203の全領域のうち、ある特定の領域のみをアクセスできるようにする。

【0024】

汎用バス122を用いてメディアプロセッサ126と通信を行う汎用プロセッサ125は汎用プロセッサ用フラッシュメモリ127を汎用プロセッサ用フラッシュメモリバス128を用いて接続されており、また汎用プロセッサ用ローカルメモリ129と汎用プロセッサ用ローカルメモリバス130を用いて接続している構成である。この汎用プロセッサ125からメディアプロセッサ126へのリードリクエストによりアクセス制御回路124が、リードするアドレスがアクセス可能であるかどうかをTLB111へTLB判定信号113を通して問い合わせる。その信号を受け取ったTLB111は設定されているアドレスと比較し、その合否をTLB合否信号114を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス109へリクエストを出し、目的のデータを引き出し、汎用バス122を通して汎用プロセッサ125へ返答する。

【0025】

また、ライトリクエストが汎用プロセッサ125からメディアプロセッサ126へ出された場合、リードリクエストと同様にアクセス可能領域であるかどうかを判定する。判定の結果、アクセス可能である場合には内部バス109を通して目的のアドレスを書き換えるが、アクセス禁止領域の場合にはライトデータは書き込まれず破棄される。

【0026】

特に、TLB111の変更はプロセッサコア101からのみ変更可能であり、汎用プロセッサ125からの変更は一切行うことができない。

【0027】

演算専用のデジタルシグナルプロセッサ（以下DSP）131に本発明を採用した実施例を図3に示す。

【0028】

DSP131は、内部バス109を持ち、その内部バス109に演算を行うプロセッサコア101、メモリインターフェース104、I/Oインターフェース105、汎用バスインターフェース123が接続されている。メモリインターフェース104はローカルメモリバス200を用いてローカルメモリ201へ接続、I/Oインターフェース105はフラッシュメモリバス202を用いてフラッシュメモリ203へ接続している。

【0029】

汎用バスインターフェース123は動作設定を行うための汎用バスインターフェースPIOレジスタ116を、プロセッサコア101はプロセッサコアPIOレジスタ117を、メモリインターフェース104はメモリインターフェースPIOレジスタ119を、I/Oインターフェース105はI/OインターフェースPIOレジスタ120を、それぞれ持っている。

【0030】

汎用バスインターフェース122にはホストCPUとなる汎用プロセッサ125が接続されており、その汎用プロセッサ125には汎用プロセッサ用フラッシュメモリ127が汎用プロセッサ用フラッシュメモリ128を用いて接続され、また汎用プロセッサ用ローカルメモリ129が汎用プロセッサ用ローカルメモリバス130を用いて接続されている。この汎用プロセッサ125から、通常全てのDSP131内部へアクセスすることが可能であり、このとき、DSP131は汎用プロセッサフラッシュメモリからプログラムをロードしてブートし、DSP131の初期設定もあわせて行う。初期設定が完了し、DSP131は内部バス109から、I/Oインターフェース105を通してフラッシュメモリ203から汎用バスインターフェース123内のTLB111の設定を行う。プロセッサコア101からのTLB書き換えリクエストを受けたTLB制御回路112はTLB更新信号115をTLB111へ出すことでTLB111内部を変更し、起動時にアクセス可能であったDSP内部と、DSP131の持つローカルメモ

リ 201 とフラッシュメモリ 203 の全領域のうち、ある特定の領域のみをアクセスできるようにする。

【0031】

この汎用プロセッサ 125 から DSP 131 へのリードリクエストによりアクセス制御回路 124 が、リードするアドレスがアクセス可能であるかどうかを TLB 111 へ TLB 判定信号 113 を通して問い合わせる。その信号を受け取った TLB 111 は設定されているアドレスと比較し、その合否を TLB 合否信号 114 を通してアクセス制御回路へ返答する。返答がアクセス可能であることを示していた場合、内部バス 109 へリクエストを出し、目的のデータを引き出し、汎用バス 122 を通して汎用プロセッサ 125 へ返答する。

【0032】

また、ライトリクエストが汎用プロセッサ 125 から DSP 131 へ出された場合、リードリクエストと同様にアクセス可能領域であるかどうかを判定する。判定の結果、アクセス可能である場合には内部バス 109 を通して目的のアドレスを書き換えるが、アクセス禁止領域の場合にはライトデータは書き込まれず破棄される。

【0033】

図 4 は外部バス 140 と内部バス 141 を接続するためのバスインターフェース回路に本発明を適応した構成図を示したものである。

【0034】

アクセス制御回路 124 は外部バス 140 と内部バス 141 へ接続されており、双方のバス間のデータ転送を行う。アクセス制御回路 124 からアクセス可能であるかどうかを調査するために照会アドレス 142 を用いて TLB 111 へ接続する。それを受けた TLB 111 はアクセス可能であるかどうかの合否判定を行い、その結果である TLB 合否信号 143 と、TLB 111 を用いてアドレス変換を行った結果のアドレス 144 をアクセス制御回路 124 へ送る。その結果を用いてアクセス制御回路は内部バス 141 へのリクエストを出力する。また、内部バス 141 を通してのみ TLB 111 は書き換え可能であるため、内部バス 141 からの TLB 更新要求を TLB 制御回路 147 が受け、TLB 更新信号 1

4 5 と T L B 1 1 1 内のどのエントリを変更するかを通知するアドレスをエントリアドレス 1 4 6 を通して、T L B 1 1 1 へ送る。送られてきたアドレスを元に T L B 1 1 1 内部を更新し、アクセスの制限を行うことが可能となる。

【 0 0 3 5 】

ここで、T L B 更新要求はプロセッサコア 1 0 1 から発行される。また、上記 T L B 更新要求は、アクセス制御回路にも送信されるが、内部バスのアドレスからアクセス制御回路と T L B 制御回路のどちらかへの要求と判断される。

【 0 0 3 6 】

図 5 は図 4 とは別の実現方法で本発明を適応した実施例を示したものである。アクセス制御回路 1 5 0 は外部バス 1 5 1 と内部バス 1 5 2 へ接続されており、双方のバス間のデータ転送を行う。許可ビット制御回路 1 6 1 は内部バス 1 5 2 に接続されたプロセッサコア等からのリクエストを随時受け付けており、外部バス 1 5 1 からのアクセスの制限を変更したい場合に要求が送られる。

まず、外部バス 1 5 1 からリード、もしくはライトリクエストにより、アドレスがアクセス制御回路 1 5 0 とアクセス判定回路 1 5 3 内部のアドレスデコーダ 1 5 4 へと送られる。アドレスデコーダ 1 5 4 へと送られたアドレスにより領域選択信号 1 5 5 をセレクタ 1 5 6 へ送る。許可ビット群 1 6 0 から許可ビット信号 1 5 8、1 5 9 を通してセレクタ 1 5 6 へ常に送られている許可ビット信号の一つを領域選択信号 1 5 5 により、その一つを選択しアクセス合否信号 1 5 7 を通してアクセス制御回路 1 5 0 へ結果を送る。ここで、ビット群は、レジスタ群に格納されたビット情報の意である。その信号を受けたアクセス制御回路 1 5 0 は要求のあったアドレスに対して破棄するかを決定し、アクセス可能領域であるならば内部バス 1 5 2 へリクエストを発生させる。

【 0 0 3 7 】

また、許可ビット群 1 6 0 の書き換えは内部バス 1 5 2 より発生した書き換え要求を許可ビット制御回路 1 6 1 へ送り、その要求によって変更するビットへ許可ビット変更信号 1 6 2、1 6 3 を通して、許可ビット群 1 6 0 を変更する。特に、許可ビット群 1 6 0 の変更は内部バス 1 5 2 からのみ変更可能であり、外部バス 1 5 1 からの変更は一切行うことができない。

【 0 0 3 8 】

図 6 は、アクセス制御のフローチャートである。まず、メディアプロセッサが起動し（4 0 0）、T L B の設定 4 0 1 を行う。T L B 初期値 4 0 2 からデータを読み出し、T L B の設定を行うが、この初期設定値はフラッシュメモリ等の不揮発性メモリに収められている。T L B の設定 4 0 1 後に、メディアプロセッサは、プログラムの読み込み 4 0 3 において、T L B 初期値 4 0 2 同様にフラッシュメモリに収められたプログラム 4 0 4 をメディアプロセッサ自身のローカルメモリへ読み出す。

【 0 0 3 9 】

そのプログラムを実行中に外部からのアクセス 4 0 5 が発生したかどうかを判定し、発生していない場合はプログラム実行を継続し、発生した場合は T L B の参照 4 0 6 を行う。T L B の参照 4 0 6 の結果、許可領域のアクセス 4 0 7 であるかどうかを判別し、許可領域ではなかった場合はそのリクエストを破棄し、プログラムの実行を継続し、外部からのアクセス 4 0 5 が発生するまで待機する。許可領域のアクセスであった場合にはデータ転送 4 0 8 を行い、リードリクエストであればメモリ 4 0 9 からデータを読み出し、ライトリクエストであればメモリ 4 0 9 へ書き込みを行う。この時のメモリ 4 0 9 はローカルメモリや内部メモリ、内部レジスタが対象となる。

【 0 0 4 0 】

T L B 内部の構造を図 7 に示す。まず、T L B 1 1 1 内部の情報を書き換えるため、T L B 更新信号 1 1 5 を受信する。T L B 更新信号 1 1 5 には T L B エントリデータ 3 0 0 と T L B アドレス 3 0 1 が含まれる。T L B アドレス 3 0 1 の信号はデコーダ 3 0 2 に送信され、デコーダ 3 0 2 で書き換えるべき T L B 1 1 1 のエントリが確定する。そのアドレスに対して、T L B エントリデータ 3 0 0 が書き込まれ、T L B 1 1 1 の内容である有効ビット 3 0 3、仮想ページ番号 3 0 4、アクセスサイズ 3 0 5 が更新される。

【 0 0 4 1 】

更新された T L B 1 1 1 内の比較器 3 1 0 では、外部からのアクセスによるアクセスアドレス 3 0 7 と T L B 1 1 1 に格納された内容と比較をする。このとき

、有効ビット 3 0 3 は有効ビット信号 3 1 1 を通して比較器 3 1 0 へ送られ、有効なエントリとのみ比較を行う。有効なエントリの仮想ページ番号 3 0 4 は、アクセスが許可されるアドレスの先頭番地を示しており、アクセスサイズ 3 0 5 を足した値が終了番地を示している。そのため、これらの信号をそれぞれ仮想ページ番号信号 3 0 8 とアクセスサイズ信号 3 0 9 として比較器 3 1 0 へ送り、アクセスアドレス 3 0 7 がその範囲内のアクセスであるか否かを判定し、比較結果 3 1 2 をエントリ毎に出力する。

【 0 0 4 2 】

エントリ毎に出力された比較結果 3 1 2 は OR 回路 3 1 3 によって論理和を取り、アクセス判定信号 3 1 4 を返す。このような回路によってアクセスの許可、不許可を決定する。

【 0 0 4 3 】

さらにアドレス変換機能を持った場合の TLB 内部の構造を図 8 に示す。TLB 1 1 1 内部の情報を書き換えるため、TLB 更新信号 1 1 5 があり、その信号は TLB エントリデータ 3 0 0 と TLB アドレス 3 0 1 の信号である。TLB アドレス 3 0 1 の信号をデコーダ 3 0 2 によって書き換えるべき TLB 1 1 1 のエントリが確定する。そのアドレスに対して、TLB エントリデータ 3 0 0 が書き込まれ、TLB 1 1 1 の内容である有効ビット 3 0 3、仮想ページ番号 3 0 4、アクセスサイズ 3 0 5、物理ページ番号 3 1 6 が更新される。尚、本実施例では、上記パラメータを更新すべきパラメータとして選択したが、常に上記パラメータの更新を要するものではない。

【 0 0 4 4 】

例えば、有効ビットを選択しない場合は、最初はすべて同じデータを物理ページ番号、アクセスサイズに入れておいて、かつ、アクセスサイズは全領域アクセス可能にすることが考えられる。

【 0 0 4 5 】

また、物理ページ番号、アクセスサイズは、始点、終点を示し、どこからどこまでをアクセスできるかを記述しているが、これらのパラメータを選択しない場合は、物理ページ領域を始点として固定領域をアクセス可能にすることも可能で

ある。

【0046】

更新されたTLB111は外部からのアクセスによるアクセスアドレス307が、比較器310でTLB111の内容と比較をする。このとき、有効ビット303を有効ビット信号311を通して比較器310へ送り、有効なエントリとのみ比較を行う。有効なエントリの仮想ページ番号304は、アクセスが許可されるアドレスの先頭番地を示しており、アクセスサイズ305を足した値が終了番地を示している。そのため、これらの信号をそれぞれ仮想ページ番号信号308とアクセスサイズ信号309として、比較器310へ送り、比較器310ではアクセスアドレス307がその範囲内をアクセスしているかを判定し、比較結果312を各エントリ毎に出力する。この信号はOR回路313と、該当するエントリの物理ページ番号を選択するセレクタ318へ送られる。OR回路313へ送られた比較結果312は論理和をとり、アクセス判定信号314を返す。また、セレクタ318では、n個ある物理ページ番号(PPN)316のうちの一つを選択し、変換後アドレス319を出力する。この変換は、外部バスからのアクセスが発生した場合、外部バス上のアドレスで行われる。そのアドレスはTLB111を搭載するプロセッサ内部のアドレスとは違うため、アドレスの変換を行う必要がある。このアドレス変換でのボトルネックを解消するために物理ページ番号への変換機能を持たせ、プロセッサ内部をアクセスできるアドレスへ高速に変換することが可能である。

【0047】

TLB111にアクセス可能領域、不可領域を設定した場合を図9に示す。TLB111内のエントリA330によってローカルメモリ334を参照可能領域に設定している。また、エントリB331によってローカルメモリ336を参照可能領域に設定している。ローカルメモリ335とローカルメモリ337はTLB111によって参照可能領域に設定されていないため、外部からのアクセスは遮断される領域となる。

【0048】

また、エントリC332によってコプロセッサ用メモリ338の領域を参照す

ることが可能である。しかし、コプロセッサ用メモリ 3 3 9 の領域は T L B 1 1 1 によって参照可能領域に設定されていないため、外部からのアクセスは遮断される。同様に、レジスタマップの領域のうち、エントリ D 3 3 3 によってレジスタマップ 3 4 1 が参照可能領域となっている。レジスタマップ 3 4 1 の前後の空間である、レジスタマップ 3 4 0 とレジスタマップ 3 4 2 は参照不可領域であり、プロセッサ外部からのアクセスは遮断され、リード、ライトすることができない。

【 0 0 4 9 】

ただし、アクセス不可領域は外部からのアクセスのみ遮断し、プロセッサ内部からは、制限なくアクセスすることができる。

【 0 0 5 0 】

また、図 1 0 には P C I のベースアドレスレジスタ（以下、B A R）を用いてメモリ空間のアクセスできる領域を制限する方法を示す。

【 0 0 5 1 】

まず、P C I の B A R を用いてメモリ空間のアクセスできる領域を制限する方法の概要を示す。

【 0 0 5 2 】

P C I デバイスには、そのデバイスが必要とするメモリ空間があり、各デバイスによってそのサイズは様々である。現在の P C I の規格では P C I は 4 G B のメモリ空間を持っているが、その空間上に、P C I デバイスのメモリ空間を割り当てている。例えば、P C I デバイス A が 0x4000 のメモリ空間を持っていたとき、P C I 空間の 0x1000 から割り当てると、P C I バス 0x1000 ~ 0x4fff をアクセスすると、P C I デバイス A のメモリ空間を操作することが可能となる。ここで、該メモリ空間を設定するときに使用するものが B A R であり、デバイス側が必要に応じて自分自身の B A R のサイズを変更できるようにするものである。具体的には、P C I デバイスは 128MB のメモリを持っていたとき、本来、P C I 空間には 128MB 分の空間を割り当てることができる。しかし、故意に 64MB しか割り当てないようにする（実現方法は図 1 0、1 1）ことで、P C I から残りの 64MB を見えないようにすることができる。

【0053】

例えば、P C Iバス上にリクエストが発生したとき、各P C IデバイスはそのリクエストのアドレスをB A Rの内容と比較し、そのアドレスが自分宛と判断したときに返答をする。つまり、P C IデバイスのP C Iインターフェースは設定されたB A Rとリクエストアドレスを比較し、自分のメモリ空間へのアクセスかを判定している。しかし、B A Rがあらかじめ64MBしかないと設定されていれば、65MBのアクセスがきたとしても、自分へのアクセスではないと判断する。

【0054】

次に、P C IのB A Rを用いてメモリ空間のアクセスできる領域を制限する具体的な方法を示す。

プロセッサの外部より入力されるB A Rの領域を指定するB A R設定信号350が、電源が投入、もしくはソフトウェアリセットや外部リセットボタンによるリセットが発生した場合等にデータ保持レジスタ354によって保持される。リセット信号351が論理値1の時にリセット期間であることを表す場合、クロック信号353とともにAND回路352に入力して論理積をとり、リセット信号351が論理値1を取ったときにデータ保持レジスタ354を更新する。保持データ355はデコーダ356によってB A Rへ送るデータが確定する。

【0055】

確定した信号は、B A R363のnビット目364、n+1ビット目365、n+2ビット目366、n+3ビット目367用にそれぞれデコード結果358、359、360、361をAND回路362へ送る。それらの信号とB A R変更信号357と論理積がとられ、その結果がB A R363のnビット目364、n+1ビット目365、n+2ビット目366、n+3ビット目367に反映される。

【0056】

この図10の方法の場合、デコーダ356からデコード結果358、359、360、361へ全て論理値1が出力されていた場合、B A R変更信号357によってnビット目364を含めた上位のビットは変更することが可能である。この領域は、P C I空間へ割り当てられる最小領域であり、メモリ空間は 2^n を

持つこととなる。このようにして、P C I 空間へ最大 $2^{(n+3)}$ の領域を割り当てることが可能である。このような設定ができるプロセッサにおいて $2^{(n+3)}$ のローカルメモリを持っていたとして、B A R へ 2^n を設定できるようにする。この場合、番地 $0 \sim (2^n - 1)$ までは P C I 空間から参照可能であるが、番地 $(2^n) \sim (2^{(n+3)} - 1)$ までは P C I 空間に割り当てられないため、外部のデバイスからは不可視となり、アクセスすることはできない。このような方法を用いてアクセスを抑制することができる。

【0057】

図10のデータ保持レジスタ354をプロセッサ内部から変更する場合を図11に示す。セクタ369を用いて選択信号370によって、データ保持レジスタ354かプロセッサ内部からのB A R 領域を指定するB A R 設定信号368を選択する。選択したデータを再度データ保持レジスタ354を更新する。保持データ355はデコーダ356によってB A R へ送るデータが確定する。確定した信号は、B A R 363のnビット目364、n+1ビット目365、n+2ビット目366、n+3ビット目367用にそれぞれデコード結果358、359、360、361をAND回路362へ送る。それらの信号とB A R 変更信号357と論理積がとられ、その結果がB A R 363のnビット目364、n+1ビット目365、n+2ビット目366、n+3ビット目367に反映される。

【0058】

つまり、ベース・アドレス・レジスタのある特定のビットを論理値0固定する機能を有するP C I バスインターフェースにおいて、ある特定のベース・アドレス・レジスタのビットを論理値0固定にすることで、P C I デバイスが持つローカルメモリよりも小さいメモリ空間を、P C I バス上のメモリ空間へ割り当て、ローカルメモリを持つP C I デバイス自身は全空間にアクセスすることが可能であるが、それ以外のP C I デバイスはP C I バス上のメモリ空間へ割り当てた小さいメモリ空間にのみアクセスできる。

【0059】

このような方法によってもB A R を変更することが可能であり、アクセス不可領域を指定することが可能である。

【0060】

本発明を採用したメディアプロセッサを搭載したセット・トップ・ボックス（以下、STB）を図12に示す。

【0061】

STB380は、メディアプロセッサ100と、ローカルメモリバス200を用いてローカルメモリ201、フラッシュメモリバス202を用いてフラッシュメモリ203、汎用バス381を用いてサービスポート382が接続、搭載されている。また、本システムはSTBであるため、映像信号の入出力を行うビデオ入出力386、音声信号の入出力を行うオーディオ入出力387、映像信号の解読などに使用する暗号鍵を保持する暗号記憶カードインターフェース信号388、外部の記憶装置と高速にデータ通信を行うための高速デジタルバス389、BSデジタルチューナから映像信号を受けるトランスポート・ストリーム・インターフェース信号390を持つ。

【0062】

また、サービスポート382は故障診断時に保守端末391を接続するためのものであり、サービスポート382と汎用インターフェース信号383を用いて接続する。汎用インターフェース信号383は保守用プロセッサ392と接続されており、保守プロセッサ自身もローカルメモリバス393を用いてローカルメモリ394が接続されている。

【0063】

保守端末391が接続された場合には、STB内部のメモリがリード、ライトできる状態ではなく、ローカルメモリ上のアクセス可能領域385のみ、読み書き可能である。ローカルメモリ上のアクセス不可領域384はSTB380に搭載されているメディアプロセッサ100からのみアクセス可能であり、保守を行う場合はアクセス可能領域385を用いてメディアプロセッサ100と通信を行うこととなる。

【0064】

このため、保守端末以外がサービスポート382へ接続され、メディアプロセッサ100内の重要なデータである、暗号解読に使用する暗号鍵や、メディアプ

ロセッサ100を動作させるソフトウェアを保護することが可能である。

【0065】

また、外部からの不正なアクセスにより、メディアプロセッサ内部の機密事項である暗号鍵やソフトウェアが格納されているメモリへのアクセスを遮断することができ、そのアクセス範囲はアプリケーションによって自由に変更可能である。尚、本実施例でアクセス制限がかかるのは物理的な領域であるが、論理的な領域について制限をかけてもよい。本発明は、上述の実施の形態に限定されるものではなく、適用分野に関わらず、要旨を逸脱しない範囲で変更し実施し得ることは述べるまでもない。

【0066】

【発明の効果】

本発明を適用することで、プロセッサ内部の機密情報や、プロセッサに接続するローカルメモリやフラッシュメモリなど外部メモリの内容を保護し、外部からの不正読み出しを防止することが可能となる。

【図面の簡単な説明】

【図1】

本発明を搭載したメディアプロセッサをP C Iバスへ接続した構成図である。

【図2】

本発明を搭載したメディアプロセッサを汎用バスへ接続した構成図である。

【図3】

本発明を搭載したD S Pを汎用バスへ接続した構成図である。

【図4】

外部バスと内部バスをT L Bを用いて接続する構成図である。

【図5】

外部バスと内部バスをアクセス制御ビット群を用いて接続する構成図である。

【図6】

アクセス制御のフローチャート図である。

【図7】

T L B内部の構成図である。

【図 8】

T L B にアドレス変換機能を持った T L B 内部の構成図である。

【図 9】

メモリやレジスタマップへの割り当てを示す図である。

【図 1 0】

B A R を用いたアクセス制御の構成図である。

【図 1 1】

B A R を用いたアクセス制御の構成図である。

【図 1 2】

本発明を搭載したメディアプロセッサを S T B に用いた構成図である。

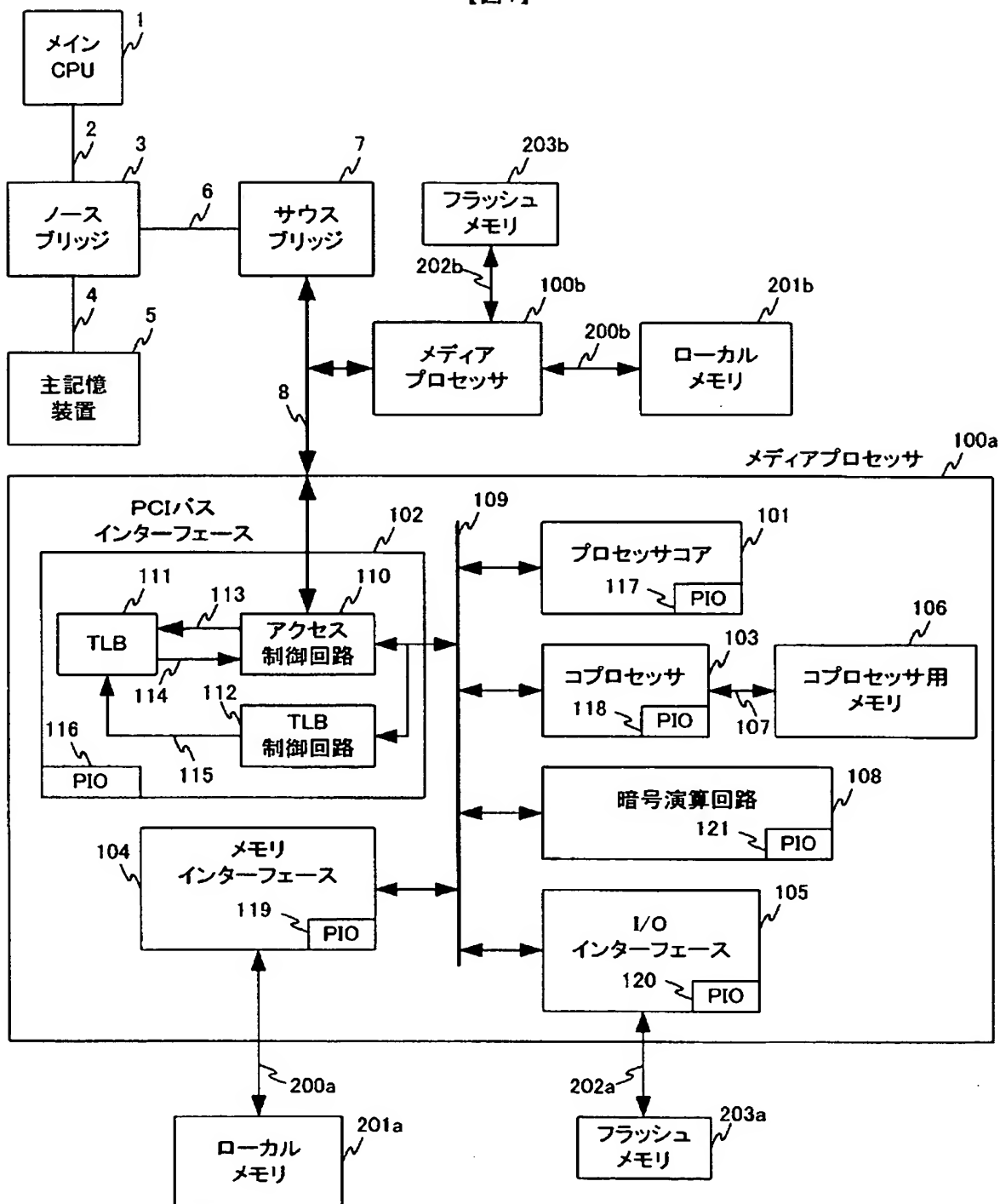
【符号の説明】

1…メイン C P U、3…ノースブリッジ、5…主記憶装置、7…サウスブリッジ、1 0 0…メディアプロセッサ、1 0 1…プロセッサコア、1 0 2…P C I バスインターフェース、1 1 0…アクセス制御回路、1 1 1…T L B、1 1 2…T L B 制御回路、1 2 5…汎用プロセッサ、1 3 1…デジタルシグナルプロセッサ、2 0 1…ローカルメモリ、2 0 3…フラッシュメモリ、3 0 3…有効ビット、3 0 4…仮想ページ番号、3 0 5…アクセスサイズ、3 1 6…物理ページ番号

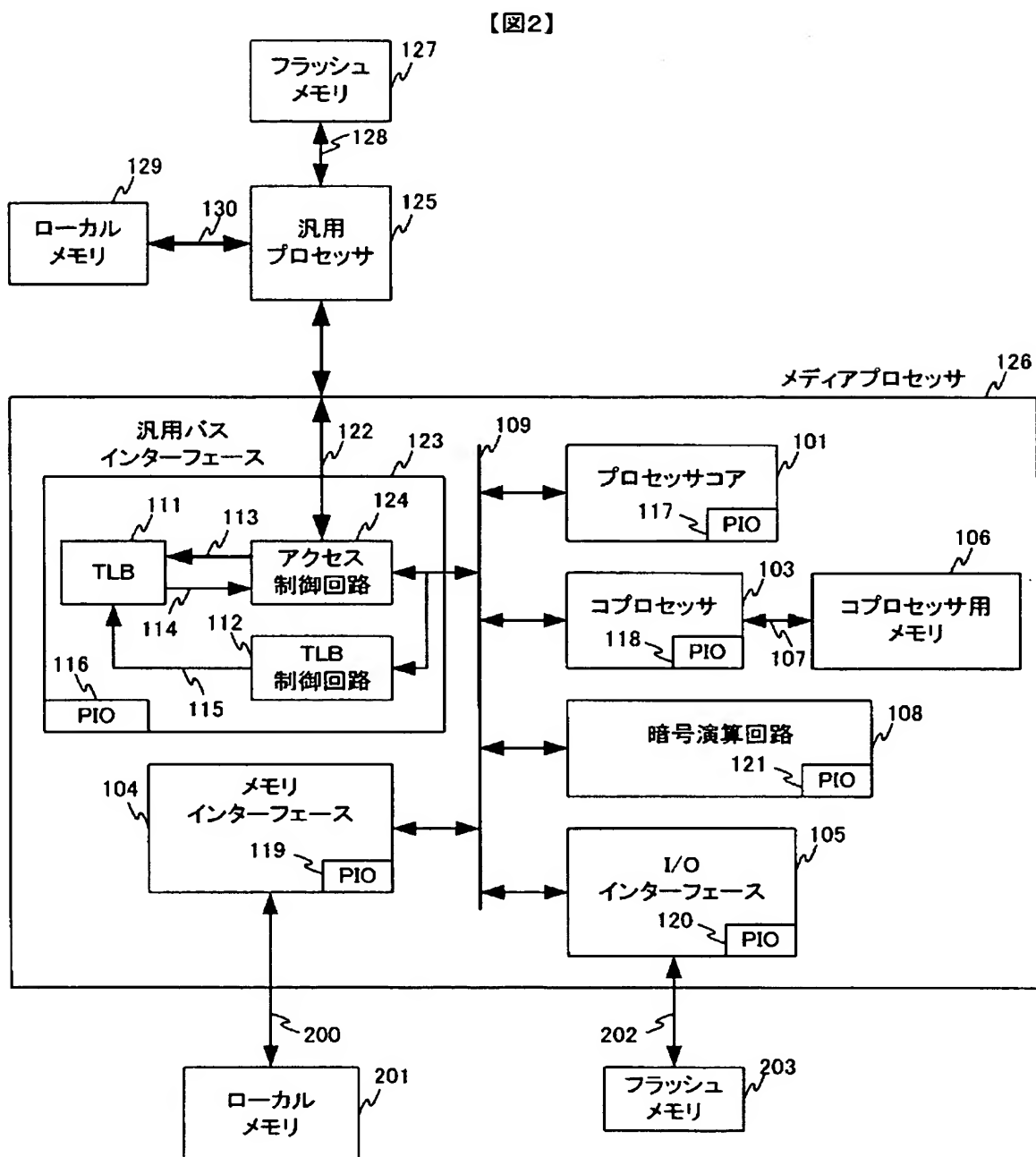
【書類名】 図面

【図 1】

【図1】

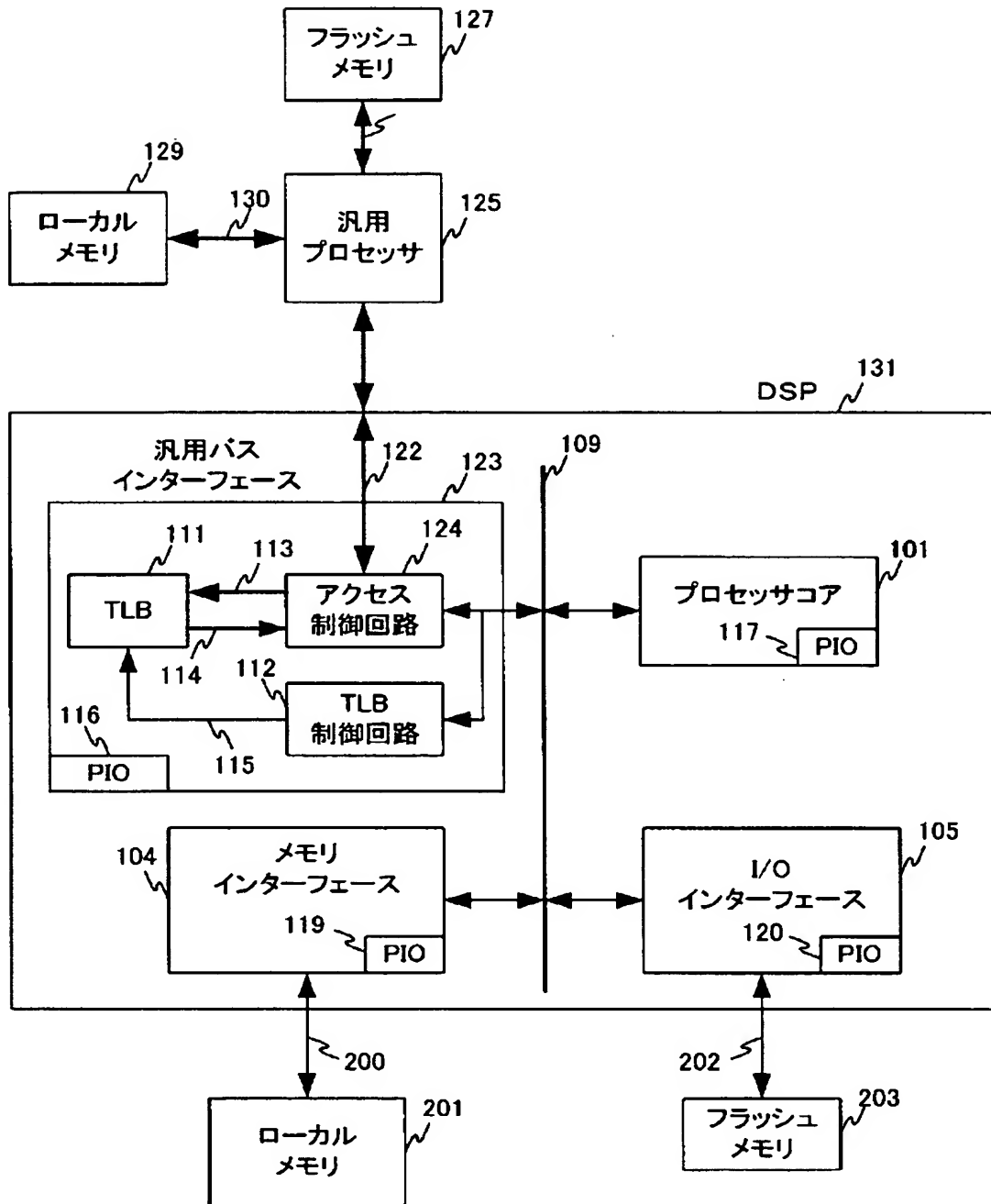


【図 2】

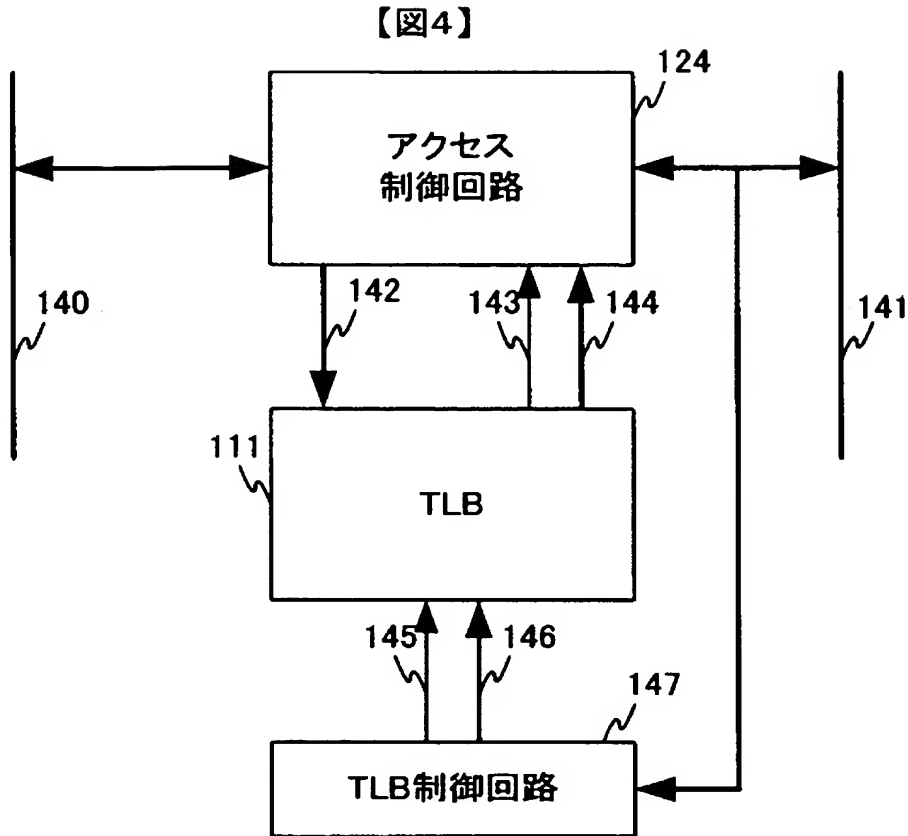


【図 3】

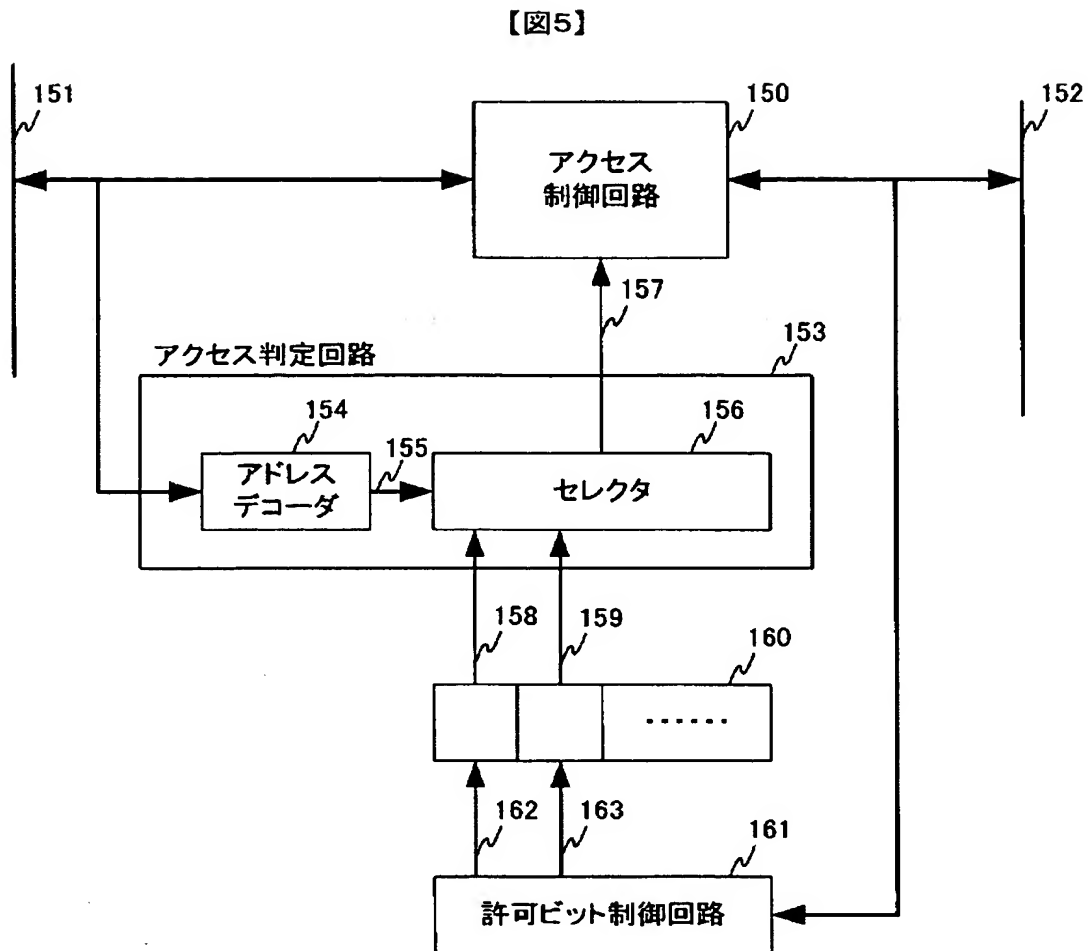
【図 3】



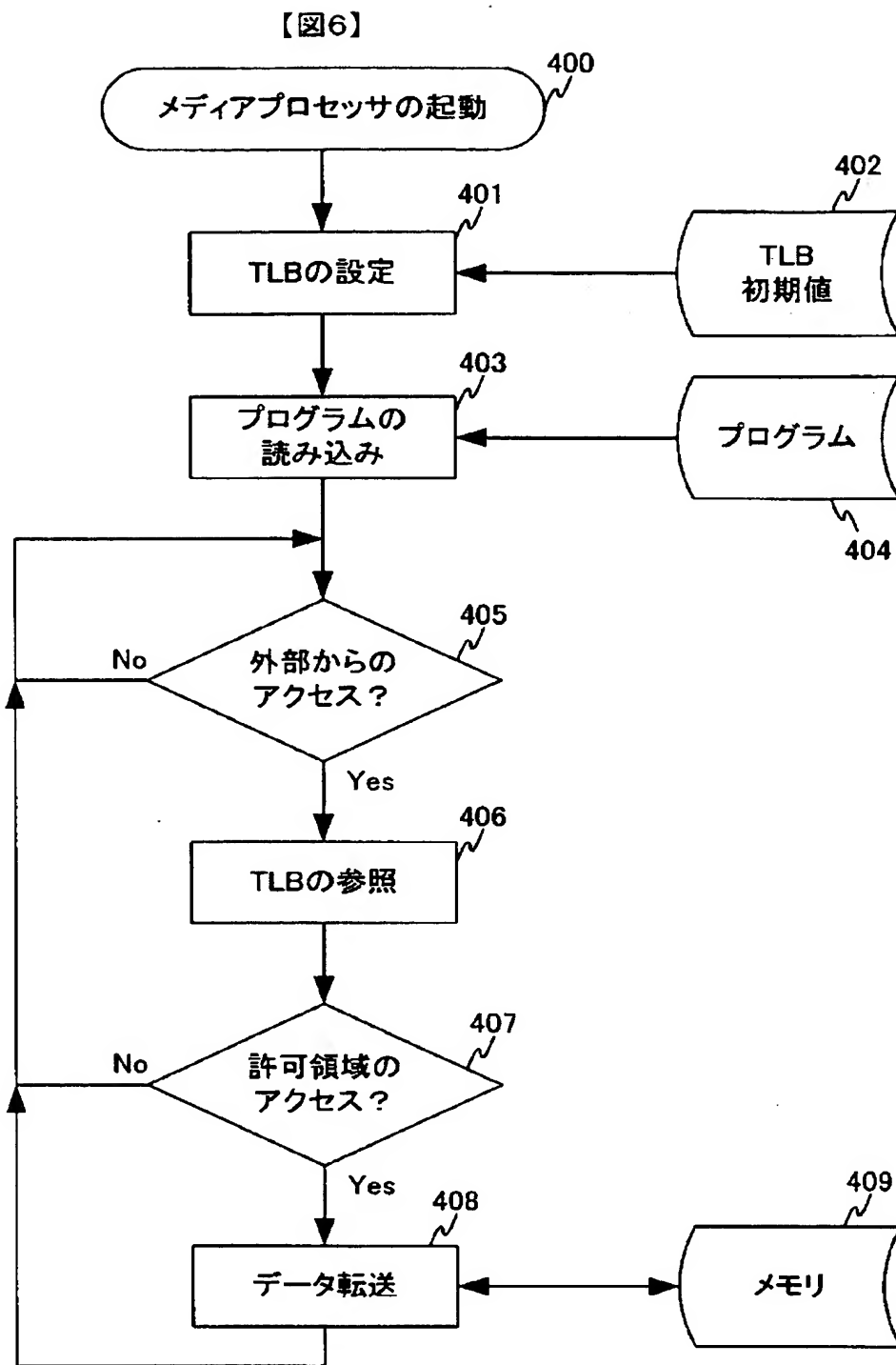
【図 4】



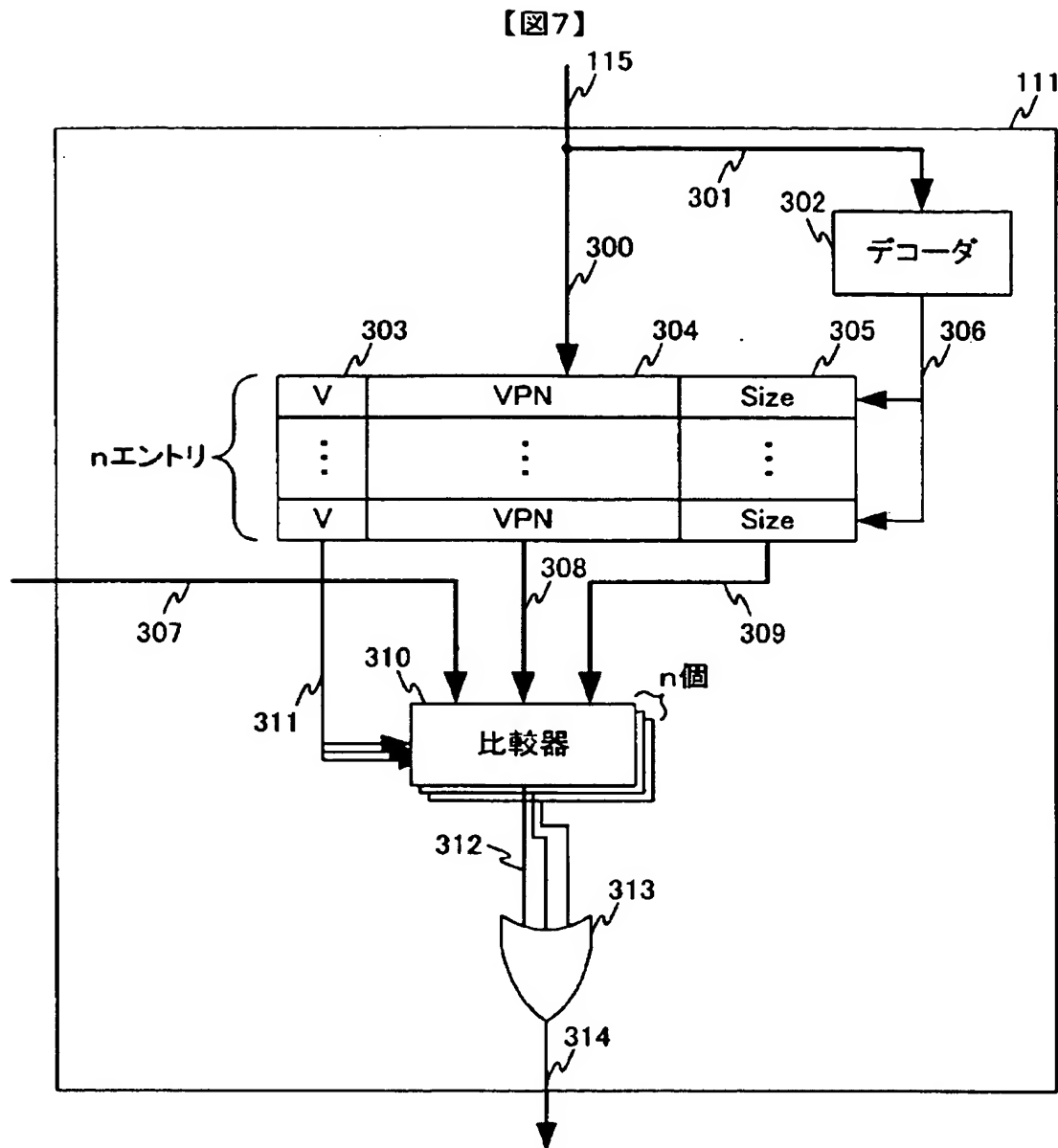
【図5】



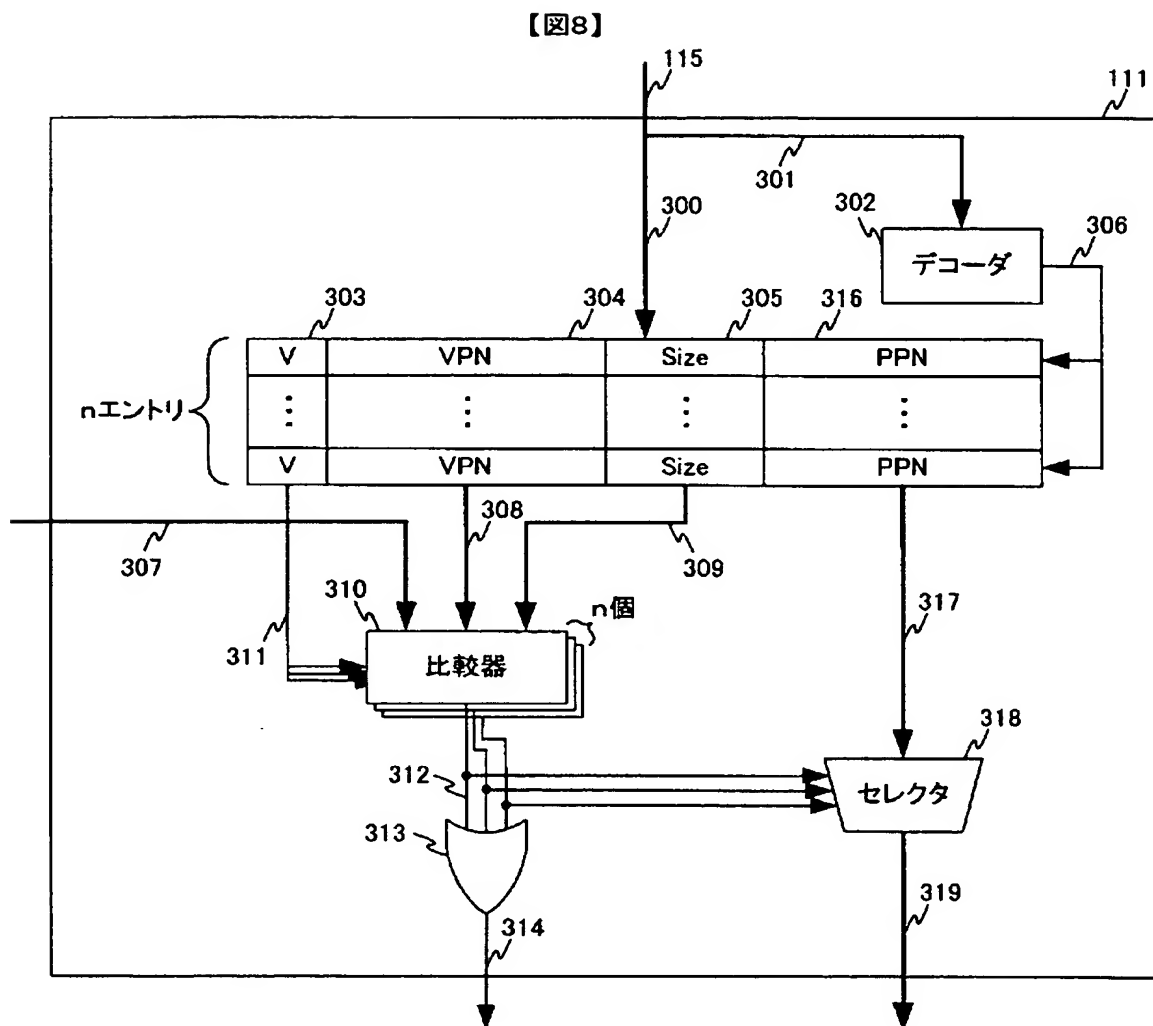
【図6】



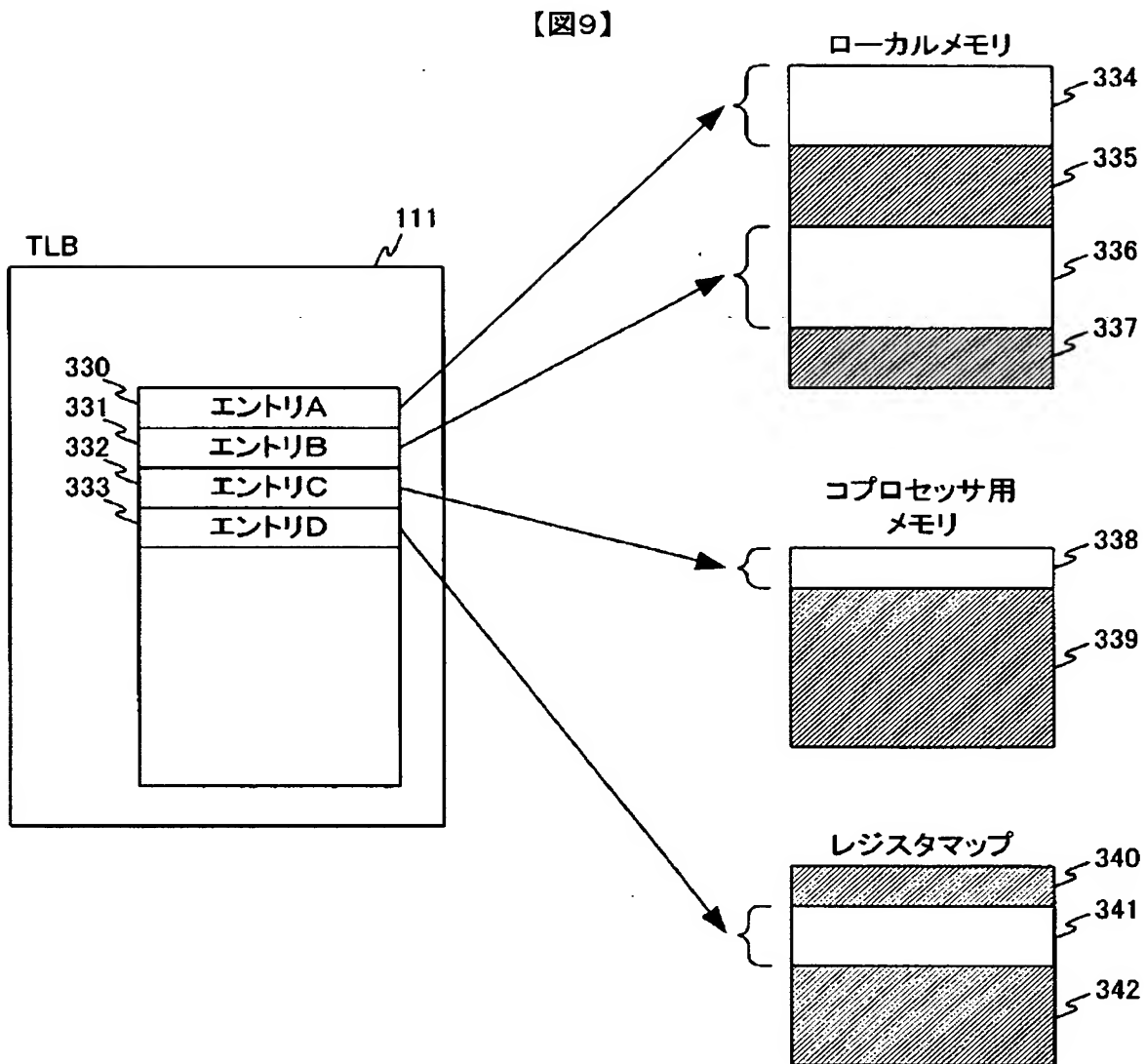
【図 7】



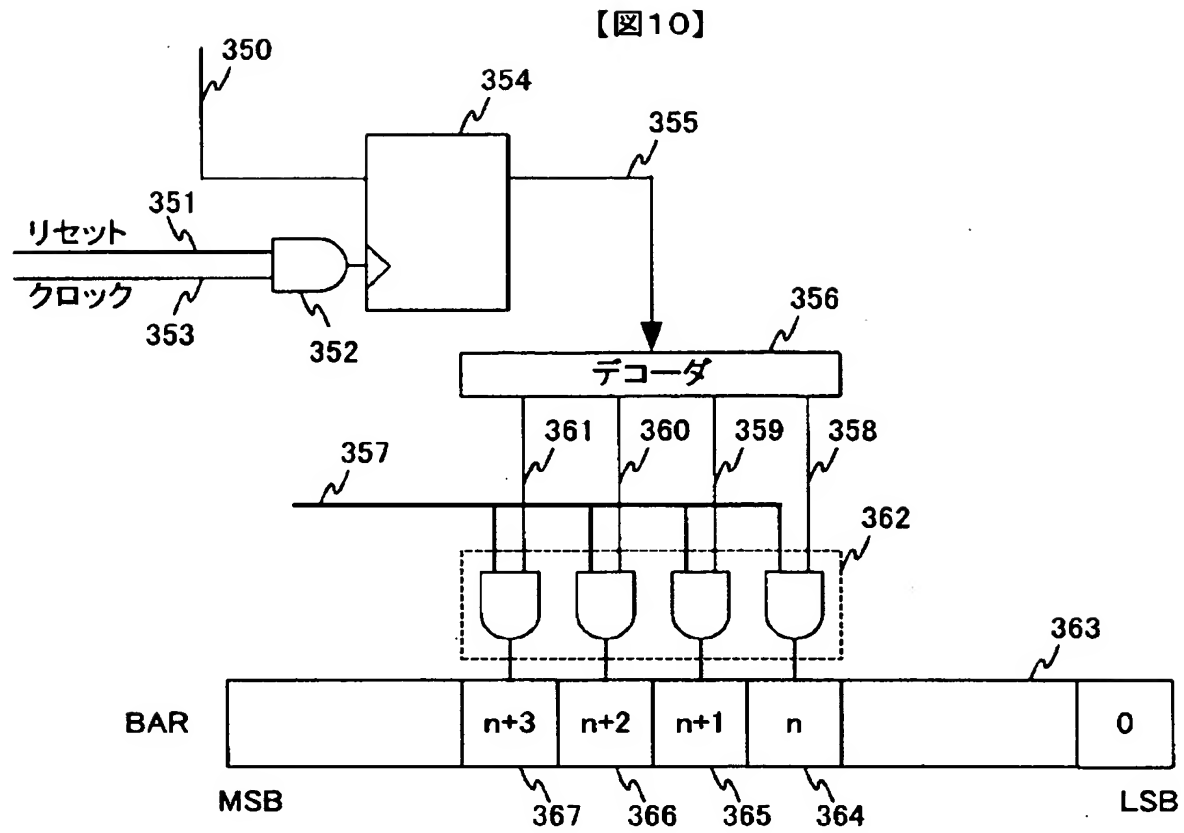
【図 8】



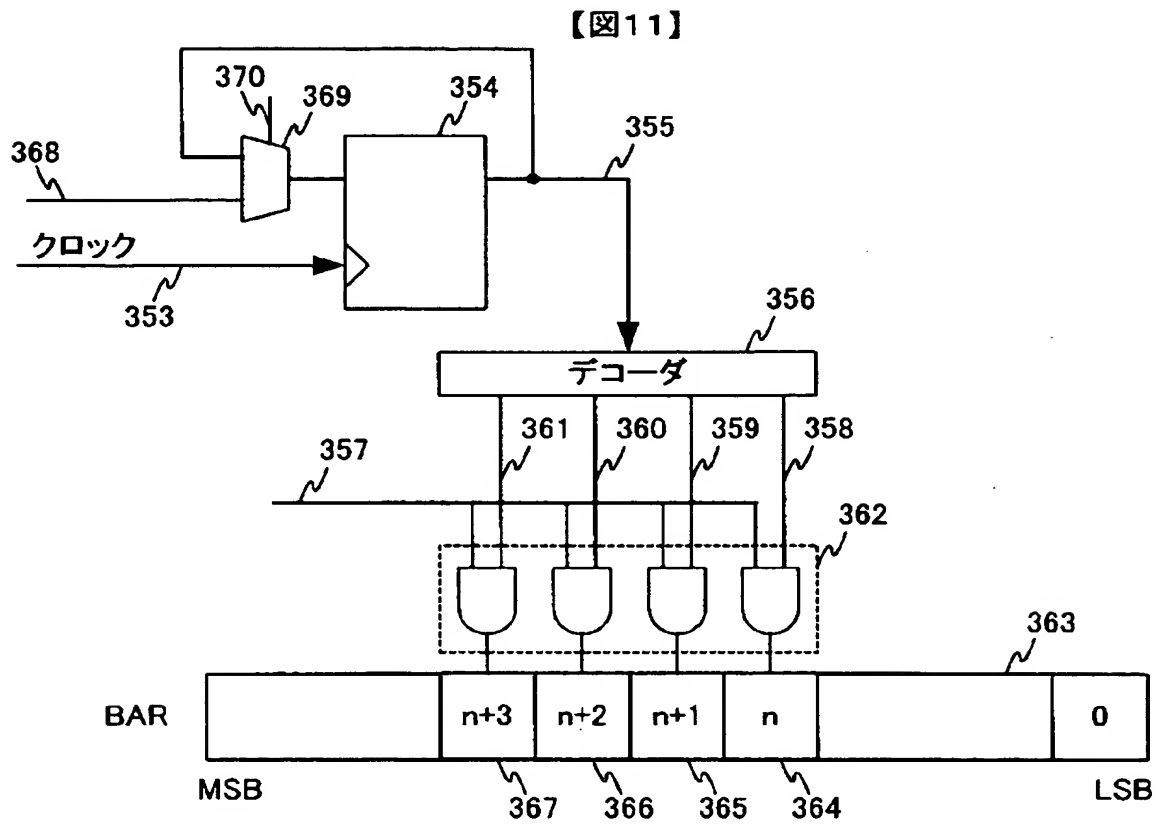
【図9】



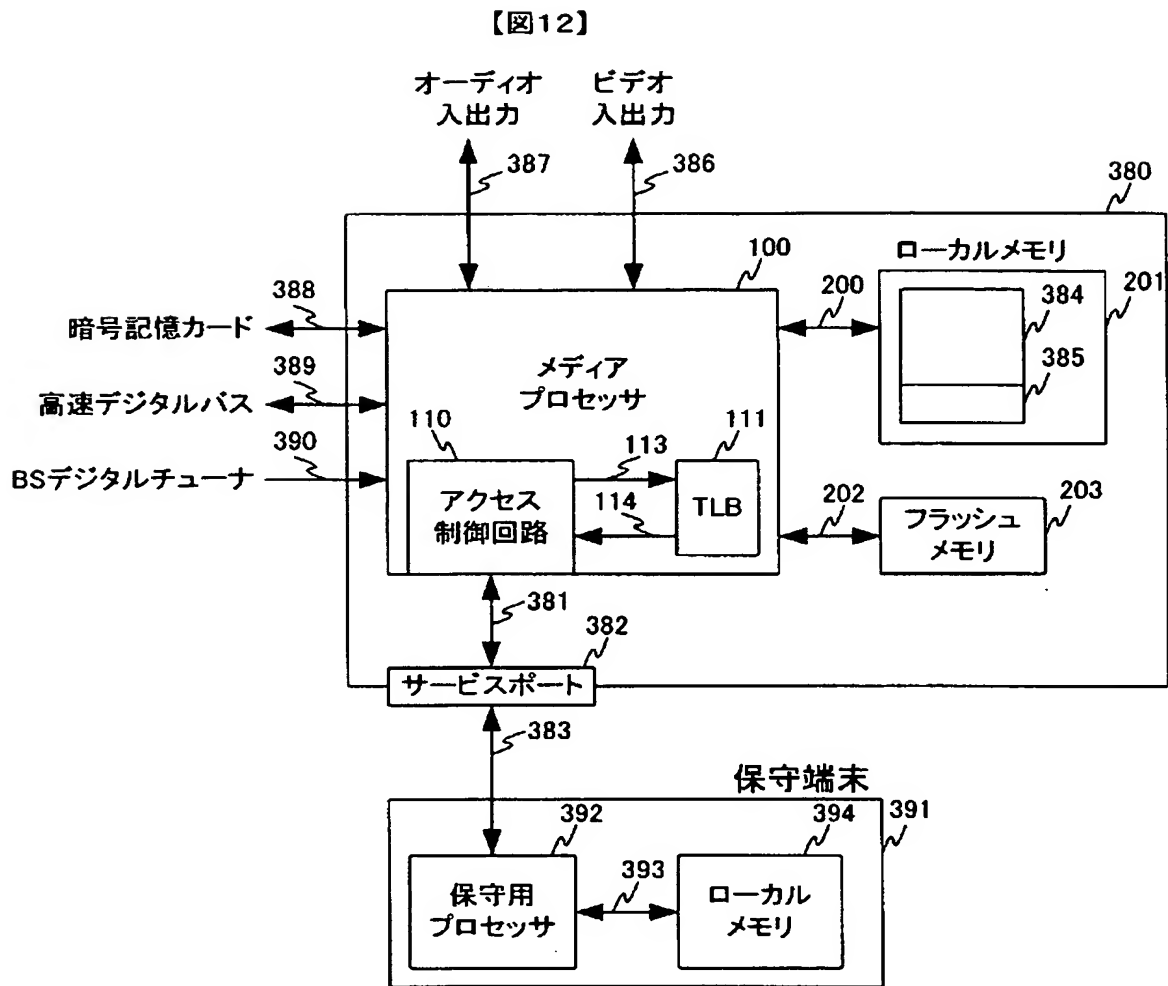
【図 10】



【図 11】



【図 12】



【書類名】 要約書**【要約】****【課題】**

外部バスからプロセッサ内部のレジスタやローカルメモリの読み出しや改変が可能であった。そのため、暗号鍵などの機密データが読み出されたり、開発したソフトウェアがコピーされてしまう可能性があった。

【解決手段】

外部と接続するバスを持つメディアプロセッサにおいて、外部バスに接続された他のデバイスからのアクセスは全て許可される。そのため、プロセッサ内部の機密事項を保護するために、メディアプロセッサのバスインターフェース部分に T L B を設け、その T L B はプロセッサ内部からのみ書き換えることができる。この T L B は外部からアクセスされたアドレスが、アクセスできるかを判定する。T L B 内にアクセス許可が記述されていればメディアプロセッサ内部へアクセスを発生し、そうでなければリクエストを破棄する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 7 2 9 1 9
受付番号	5 0 3 0 0 4 3 6 5 3 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 3 月 1 9 日

< 認定情報・付加情報 >

【提出日】 平成15年 3月18日

次頁無

【書類名】 出願人名義変更届（一般承継）

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2003- 72919

【承継人】

【識別番号】 503121103

【氏名又は名称】 株式会社ルネサステクノロジ

【承継人代理人】

【識別番号】 100080001

【弁理士】

【氏名又は名称】 筒井 大和

【提出物件の目録】

【包括委任状番号】 0308729

【物件名】 承継人であることを証明する登記簿謄本 1

【援用の表示】 特許第 3 1 5 4 5 4 2 号 平成 1 5 年 4 月 1 1 日付け
提出の会社分割による特許権移転登録申請書 を援用
する

【物件名】 権利の承継を証明する承継証明書 1

【援用の表示】 特願平 1 - 2 5 1 8 8 9 号 同日提出の出願人
名義変更届（一般承継）を援用する

【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 7 2 9 1 9
受付番号	5 0 3 0 1 4 0 3 5 2 5
書類名	出願人名義変更届 (一般承継)
担当官	伊藤 雅美 2 1 3 2
作成日	平成 1 5 年 1 1 月 4 日

< 認定情報・付加情報 >

【提出日】 平成15年 8月26日

特願 2 0 0 3 - 0 7 2 9 1 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所

特願 2 0 0 3 - 0 7 2 9 1 9

出 願 人 履 歴 情 報

識別番号

[5 0 3 1 2 1 1 0 3]

1. 変更年月日

2 0 0 3 年 4 月 1 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内二丁目 4 番 1 号

氏 名

株式会社ルネサステクノロジ